UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,601	01/23/2004	Daniel Bleichenbacher	5	7709

46303   7590   02/23/2009
RYAN, MASON & LEWIS, LLP
1300 POST ROAD, SUITE 205
FAIRFIELD, CT 96824

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _23 December 2008_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,3-13,15 and 16_ is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,3-13,15 and 16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _3/5/2004_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
  Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Currently pending claims are 1, 3 – 13, 15 and 16.

Claim Objections

2.   Claim 1 is objected to because of the following informalities: "v_{I+1}" should be presented in a more readable form to avoid being printed as "v_{I-1}" in the future upon allowance. Appropriate correction(s) is (are) required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3.   Claim 1 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter by imposing meaningful limits or significant steps properly tied to a particular machine, and therefore do not qualify as a statutory process.   The recited method claim(s) including steps of computing, establishing and generating is (are) broad enough that the claim could be

completely performed mentally, verbally or without a machine nor is any transformation

apparent. Any other claims not addressed are rejected by virtue of their dependency.

Likewise, any other independent <u>method</u> claims such as claim 3, 8, 10 or 11 that also

requires to be corrected with the same rationale set forth as above.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite because

(a) the definition (including, at least, what type of numerical values – e.g., positive integer) of u_i

and v_i are never recited and defined in the claim, (b) omitting essential elements since,

according to the specification (SPEC: Page 5 Line 13 – 17), the recited claim limitations are

valid only under the condition of gcd(s, n) ≠1.

Likewise, any other independent <u>method</u> claims such as claim 3, 10 or 13 that also

requires to be corrected with the same rationale set forth as above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in
> this country, more than one year prior to the date of application for patent in the United States.

5.   Claims 1, 3 – 13, 15 and 16 are rejected under 35 U.S.C. 102(b) as being anticipated by

Takaragi et al. (U.S. Patent 6,141,421).

As per claim 1 and 13, Takaragi discloses: generating a compressed Rabin signature based on a continued fraction expansion of s/n (Column 14, lines 21-32 Column 15, Lines 9-15); computing principal convergents, u_i / v_i, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined (Fig. 3-4, Column 8, Lines 3-5); establishing an index I, such that $v_I < (n)^{(1/2)} < v_{I+1}$ (Fig. 3 Column 8, Lines 6-20); and generating a compressed Rabin signature (vt, m) for a message, m (Fig. 3 Column 8, Lines 21-28).

As per claim 8 and 15, Takaragi discloses: applying a message formatting function, h, to the message, m, to computing h(m) (Column 10, Lines 27-50); computing a value, t, as h(m)v2 mod n (Column 10, Lines 50-65, Column 14, Lines 32-57); obtaining a value, w, as a square root of the value, t (Column 11, Lines 1-24);
computing a signature value, s, as w/v mod n; and providing a decompressed signature (s,m) (Column 11, Lines 1-24).

As per claim 10, Takaragi discloses: computing principal convergent, ui/vi, of a continued fraction expansion of s/n (Fig. 3-4, Column 8, Lines 3-5); establishing an index/, such that $v_I < (n)^{(1/2)} < v_{I+1}$ (Fig. 3 Column 8, Lines 6-20); and generating a compressed Rabin signature (vt, m) (Fig. 3 Column 8, Lines 21-28).

As per claim 11, Takaragi discloses: applying a message formatting function, h, to the message, m, to computing h(m) (Column 10, Lines 27-50); computing a value, t, as h(m)v^e mod n (Column 10, Lines 50-65, Column 14, Lines 32-57); determining whether the values t or

t-n have an eth root over integer values (Column 11, Lines 1- 24); computing a value, w, as the eth root; and computing the decompressed signature (w/v mod n, m) (Column 11, Lines 1-24).

As per claim 3, Takaragi discloses: computing principal convergent, ui/vi, of a continued fraction expansion of s/n (Fig. 3-4, Column 8, Lines 3-5); establishing an index/, such that $v_l <$ $(n)^{(1/2)} < v_{l+1}$ (Fig. 3 Column 8, Lines 6-20); and generating a compressed Rabin signature (vt, m) (Fig. 3 Column 8, Lines 21-28).

As per claim 4, rejected as applied to claim 3. Takaragi discloses: wherein sv=u(mod n) (Column 8, lines 11).

As per claim 5, rejected as applied to claim 3. Takaragi discloses: wherein lvl= square root (n) (Column 8, Lines 6-20).

As per claim 6, rejected as applied to claim 3. Takaragi discloses: wherein lul= square root (n) (Column 8, Lines 6-20).

As per claim 7, rejected as applied to claim 1. Takaragi discloses: wherein said principal convergents, ui/vi, are computer for i equal to 1 to k, where k is a largest integer for which principal convergents are defined (Fig. 3-4, Column 8, Lines 3-5).

As per claim 9, 12 and 16, rejected as applied to claim 8, 11 and 15. Takaragi discloses: comprising the step of generating an error if no integer square root exists, because it is obvious since decimal numbers are not excepted by the algorithm.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Examiner, Art Unit 2431
12/30/2008